CLAIMS

What is claimed is :

1 A post issuance system for performing data or configuration changes within a PSD, said system comprising

- said PSD, including at least one functional application and PSD cryptographic means,

- a local client functionally connected to said PSD,

- a first server functionally connected to said local client, said PSD and said first server comprising first means for mutual authentication.

- at least one HSM, including HSM cryptographic means complementary to said PSD cryptographic means, said at least one HSM being functionally connected to said first server,

- a communications pipe, established between said PSD and said at least one HSM,

- storing means for storing or generating said data or configuration changes, said storing means being functionally connected to said first server,

- said at least one HSM comprising controlling means for controlling said data or configuration changes sent through said communications pipe to said PSD.

2. The system according to claim 1 comprising a network for the establishment of said communications pipe

3. The system according to claim 1 wherein said at least one functional application includes means for processing APDU commands and said data or configuration changes received through said communications pipe.

4 The system according to claim 1 further including at least one second server in processing communications with said first server, wherein said at least one second

server includes stored data or configuration changes retrievable using a PSD unique identifier.

5 The system according to claim 4 wherein said first server and said at least one second server comprise means for mutual authentication

6 The system according to claim 1 wherein said at least one functional application includes an application identifier

7. The system according to claim 6 comprising selecting means for selecting said at least one functional application using said application identifier.

8. The system according to claim 4 comprising a network for the establishment of said communications pipe and for functionally connecting said at least one second server to said first server, and sending means for sending said retrieved data or configuration changes from said at least one second server over said network to said first server.

9. The system according to claim 4 wherein said first server comprises first processing means for receiving and processing said data or configuration changes, and wherein said at least one HSM comprises second processing means for further processing said data or configuration changes.

10. The system according to claim 1 wherein said at least one HSM comprises generating means for generating at least one command executable by said at least one functional application.

11. The system according to claim 10 wherein said at least one HSM comprises encrypting means for encrypting said at least one command and said data or configuration changes, forming at least one cryptogram.

12. The system according to claim 11 comprising sending means for sending said at least oné cryptogram through said communications pipe into said PSD for processing by said at least one functional application

13. The system according to claim 12 wherein said at least one functional application comprises decrypting means for decrypting said cryptogram using said PSD cryptographic means, and executing means for executing said at least one command.

14. The system according to claim 2 wherein said network is a public network

15 The system according to claim 2 wherein said network is a private network

16. The system according to claim 1 wherein said communications pipe is provided with a secure communications protocol.

17 The system according to claim 1 wherein said HSM cryptographic means and said PSD cryptographic means comprise complementary asymmetric keys.

18. The system according to claim 1 wherein said HSM cryptographic means and said PSD cryptographic means comprise complementary symmetric keys.

19. A post issuance method for performing data or configuration changes within a PSD, said method comprising ·

- establishing a communications pipe between said PSD and at least one HSM, wherein said PSD is functionally connected to a local client and said at least one HSM is functionally connected to a first server,

- mutually authenticating said PSD and said first server,

- selecting at least one functional application within said PSD associated with said existing data or configurations.

- generating or retrieving HSM cryptographic means complementary to cryptographic means included inside said PSD

- retrieving said data or configuration changes.

- processing said data or configuration changes by said first server,

- encrypting said processed data or configuration changes by said at least one HSM using said complementary HSM cryptographic means,

- routing said encrypted processed data or configuration changes through said communications pipe into said PSD, and

- decrypting and processing said processed data or configuration changes by said at least one functional application using said PSD cryptographic means.

20 The method according to claim 19, comprising the step of retrieving said data or configuration changes from at least one second server, and of sending said data and configuration changes over a network from said second server to said first server.

21 The method according to claim 19 further including the step of mutually authenticating said at least one second server and said first server.

22. The method according to claim 21, comprising the further step of using a unique identifier associated with said PSD for mutually authenticating said PSD and said first server.

23 The method according to claim 19, comprising the further step of using a unique identifier associated with said PSD for selecting said at least one functional application.

24. The method according to claim 19, comprising the further step of using a unique identifier associated with said PSD for generating or retrieving said HSM cryptographic means.

25. The method according to claim 19, comprising the further step of using a unique identifier associated with said PSD for retrieving said data or configuration changes.

26 The method according to claim 19, wherein at least one command executable by said at least one functional application is issued by said at least one HSM, routed

through said communications pipe into said PSD, and processed by said at least one functional application.

27 The method according to claim 19 comprising the step of functionally connecting said local client and said first server through a private network

28 The method according to claim 19 comprising the step of functionally connecting said local client and said first server through a public network.

29. The method according to claim 19 comprising the step of employing asymmetric cryptographic means for said HSM cryptographic means and said PSD cryptographic means

30. The method according to claim 19 comprising the step of employing symmetric cryptographic means for said HSM cryptographic means and said PSD cryptographic means.

31. The method according to claim 19 comprising the step of using a secure communications protocol for said communications pipe.